Bayesian Classifiers in Intrusion Detection Systems

Mardini-Bovea Johan; De-La-Hoz-Franco Emiro; Molina-Estren Diego; Paola Ariza-Colpas; Ortíz Andrés; Ortega Julio; César A. R. Cárdenas; Carlos Collazos-Morales

Abstract

To be able to identify computer attacks, detection systems that are based on faults are not dependent on data base upgrades unlike the ones based on misuse. The first type of systems mentioned generate a knowledge pattern from which the usual and unusual traffic is distinguished. Within computer networks, different classification traffic techniques have been implemented in intruder detection systems based on abnormalities. These try to improve the measurement that assess the performance quality of classifiers and reduce computational cost. In this research work, a comparative analysis of the obtained results is carried out after implementing different selection techniques such as Info.Gain, Gain ratio and Relief as well as Bayesian (Naïve Bayes and Bayesians Networks). Hence, 97.6% of right answers were got with 13 features. Likewise, through the implementation of both load balanced methods and attributes normalization and choice, it was also possible to diminish the number of features used in the ID classification process. Also, a reduced computational expense was achieved.

Keywords

Naïve bayes, Bayesian networks, Feature selection, IDS